Donyx DRM
Superuser's guide

Table of contents

1. Introduction **3**
1.1. About This Guide 3
1.2. General Information and Functions 4
1.3. Web Interface Overview 5
2. Access Levels **6**
3. Functional Capabilities **6**
4. Security **7**
4.1. Security Profile Hierarchy 7
4.2. Creating a Security Profile 8
5. Domains **12**
5.1. New Domain 12
5.2. Domain Editing 13
5.3. Domain Administrator 14
5.4. Editing a Domain Administrator 15
6. Users **16**
6.1. **Superusers** 16
6.2. New Superuser 17
6.3. Editing a Superuser 18
6.4. **Logs** 19
7. Notifications **21**
7.1. New Notification rule 22
7.2. Editing a Notification Rule 23
7.3. Notification provider (Delivery method) 23
7.4. Editing a Notification Delivery Method 24
8. Infrastructure **25**
8.1. **Firmware** (Cloud only) 26
8.2. New Firmware 27
8.3. Editing a Firmware Rule 28
9. Statistics **29**
10. Account Management **30**
11. Customer Support **31**

1. Introduction

1.1. About This Guide

This guide describes the administrative capabilities of the Donyx DRM system available to superusers.

It provides an overview of the interface and instructions for domain management, security policy configuration, and other administrative functions.

This manual covers only superuser functions. For information about basic features available to all users, see the *Donyx DRM User's Guide*.

1.2. General Information and Functions

The DRM system is designed for centralized configuration management of Donyx routers, enabling monitoring of network equipment and infrastructure status.

The DRM system provides the following core functionality:

- Monitor the status of device groups or individual Donyx routers. The user has access to information such as device status (online/offline), last response time, uptime, and data on CPU usage, LAN interfaces, loopback, routing, etc.
- Centralized firmware update for individual routers or groups of devices within the same hardware series.
- Send reboot and factory reset commands to routers. The built-in scheduler allows for configuring command execution intervals.
- Create rules for generating device backups and system logs.
- Manage configurations of routers connected to the system.

All system operations are performed remotely via a web interface accessible through a browser at drm.donyx.com. The client component is preinstalled in the router firmware.

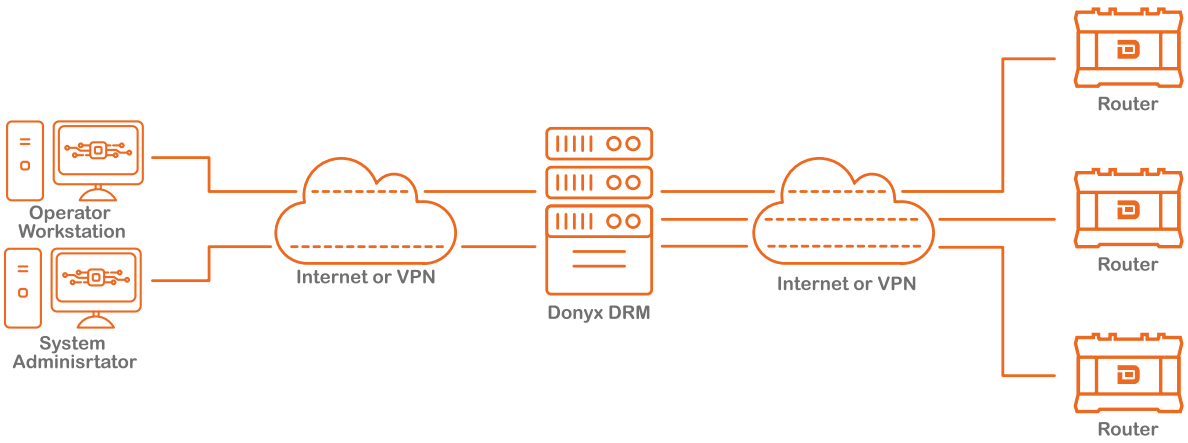


Figure 1. Organization Principle of the Donyx DRM Router Management System

The modular architecture of the Donyx DRM system allows for functionality customization to align with specific business objectives.

The **DRM** system version number is displayed within the profile editing menu. It is located in the bottom-left corner of the screen. For detailed information, refer to the **Account** section of this guide.

1.3. Web Interface Overview

The system is managed through the web interface.

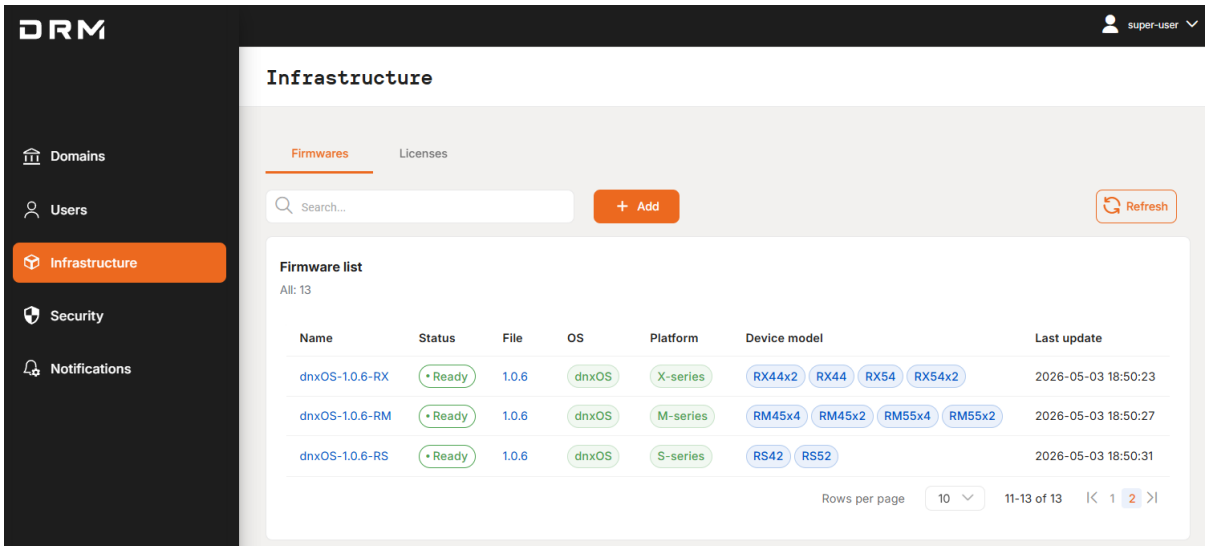
Primary navigation elements are located in the sidebar on the left side of the screen. Related sections are categorized into logical groups for efficient navigation:

- **Users:** Superusers, Logs.
- **Infrastructure:** Licenses, Firmware.

The following sections are also accessible from the sidebar:

- Security
- Domains
- Notifications

To access the **Statistics** section, click the corresponding button in the top-right corner of the screen.



The  icon for editing the user profile is located in the upper-right corner of the screen.

2. Access Levels

The DRM system uses a two-tier role structure designed to separate global system management from individual device operations.

Global System Administration: Managed exclusively by the *Superuser* role. This tier includes high-level infrastructure configuration and domain management.

Device Management: Performed by roles responsible for operations within specific domains, including *Administrator*, *Assistant*, and *Operator*.

This guide covers global system administration. Detailed information about device-level operations is available in the *Donyx DRM User's Guide*.

In cloud-based deployments, global system administration (*Superuser* access) is managed by the service provider and is not available to the end user.

3. Functional Capabilities

System installation involves the creation of a **Superuser** account. By default, the following credentials are assigned:

- Login: *root*
- Password: *root*

A strong password should be established during the initial login.

The **Superuser** performs the following functions.

- Domain creation and administration.
- Security profile creation and administration.
- Creation and configuration of additional **Superuser** accounts.
- Configuration of notification delivery methods.

4. Security

The **Security** tab displays a list of existing security profiles. A security profile defines authorization parameters and governs account behavior.

Only **Superusers** can create, edit, or delete security profiles.

4.1. Security Profile Hierarchy

The DRM system implements three levels of security profiles:

- Global (system-wide);
- Domain security profile;
- User security profile.

All security profiles created by superusers are displayed in the **Security** tab. Any profile can be assigned as a domain or user security profile during configuration.

Global Security Profile

The global security profile is created automatically and cannot be edited or deleted. This profile is named *default*. It is automatically assigned to superusers or domains during creation if no other profile is specified. The profile is not displayed in the general list of security profiles, as it is a non-editable system default.

Domain Security Profile

A profile assigned as the domain security profile is identified within the domain as *domain default*. When creating domain users, this profile is this profile is assigned by default. It is also applied if a user's assigned security profile is deleted.

User Security Profile

A security profile is assigned to a user during account creation. The user security profile takes precedence over the domain security profile.

The *domain default* profile is applied to a user in the following cases:

- if it is explicitly assigned as the user's security profile;
- if the user's individual security profile has been deleted.

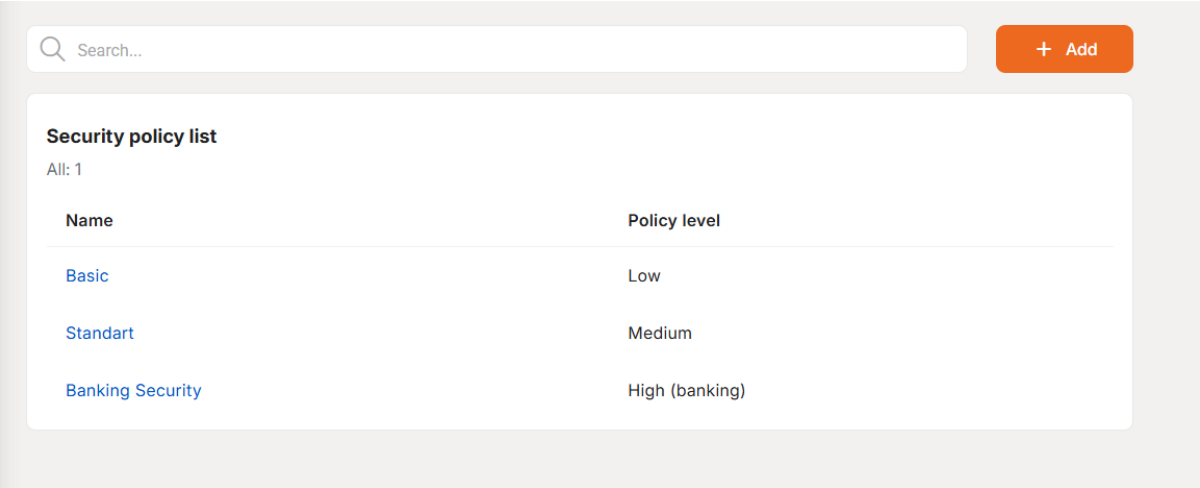
The security profile specified in the user's settings is applied during authorization.



The superuser creates only *Domain Administrator* accounts. Instructions for creating and managing other user roles are provided in the *Donyx DRM User's Guide*.

4.2. Creating a Security Profile

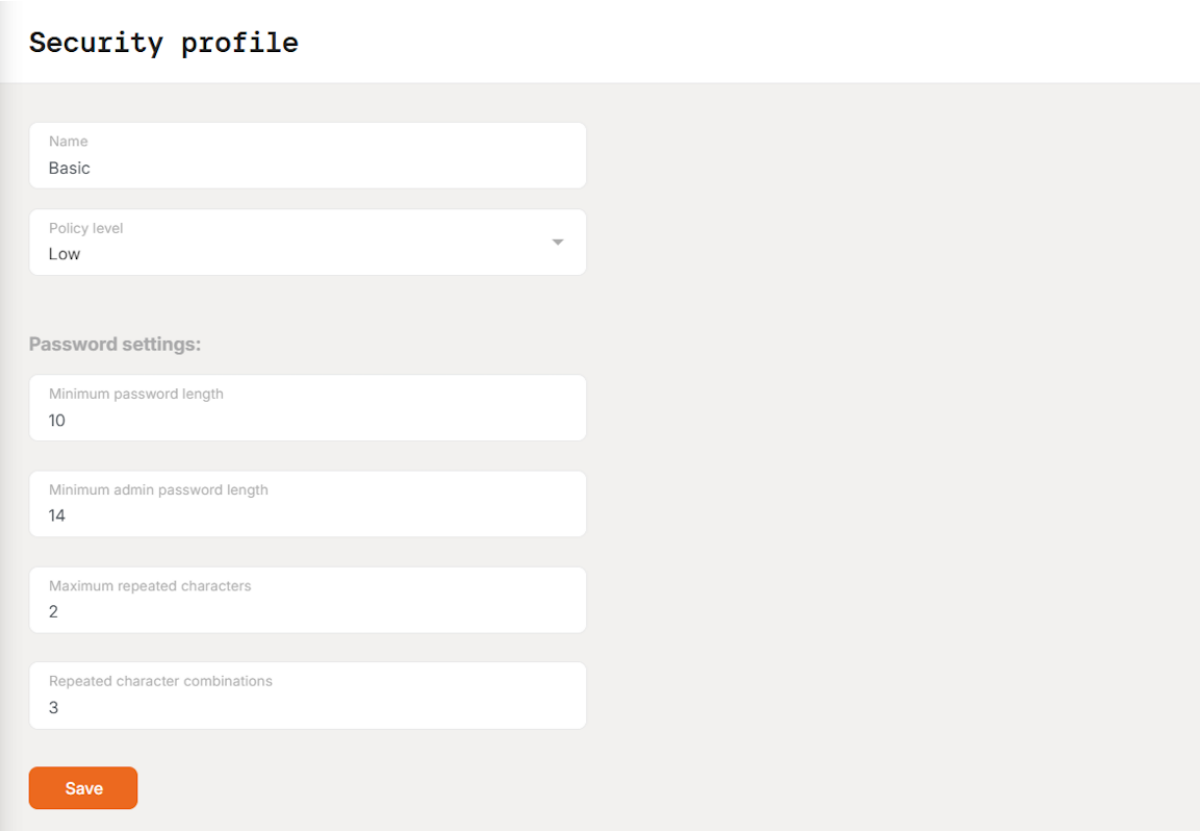
The figure below illustrates the general view of the **Security** tab.



To create a new security profile, click the 

icon. The profile creation page is displayed.

The available set of configuration parameters depends on the selected security level.



In the **Name** field, enter the identifier for the new security profile. In the **Policy level** field, select one of the following options: *Low*, *Medium*, or *High (banking)*.

Low Security Level

At the **Low** security level, a single configuration block is available: **Password settings**. By default, these fields are pre-filled with recommended values. Parameters may be modified according to specific requirements.

Table 1. Security Profile Parameters: Low Level

Field	Description
Name	Specified by the user.
Policy level	*Low* (selected from the dropdown menu).
Password settings:	
Minimum password length	Defines the minimum number of characters required for a user password.
Minimum admin password length	Defines the minimum number of characters required for passwords of accounts with administrative privileges.
Maximum repeated characters	Specifies the maximum allowed number of identical consecutive characters (e.g., if set to *2*, "aaa" is prohibited).
Repeated character combination	Specifies the maximum allowed length of a recurring sequence of characters within the password.



It is not recommended to set parameter values below the system defaults.

After completing all fields, click the **Save** button.

Medium Security Level

At the **Medium** security level, the following configuration blocks are available: **Password settings**, **Authentication settings**, and **Two-factor authentication**. By default, some fields are pre-filled with recommended values. Parameters may be modified according to specific requirements.

Table 2. Security Profile Parameters: Medium Level

Field	Description
Name	Specified by the user.
Policy level	*Medium* (selected from the dropdown menu).
Password settings:	
Minimum password length	Defines the minimum number of characters required for a user password.
Minimum admin password length	Defines the minimum number of characters required for passwords of accounts with administrative privileges.
Maximum repeated characters	Specifies the maximum allowed number of identical consecutive characters (e.g., if set to *2*, "aaa" is prohibited).
Repeated character combination	Specifies the maximum allowed length of a recurring sequence of characters within the password.
Authentication settings:	
Attempts before temporary lockout	The maximum number of failed login attempts allowed before the account is temporarily suspended.
Attempts before permanent lockout	The cumulative number of failed login attempts allowed before the account is permanently blocked.
Temporary lockout duration (minutes)	The duration, in minutes, for which the account remains suspended after exceeding the temporary attempt limit.
User password expiration (days)	The validity period of a standard user password in days.

Admin password expiration (days)	The validity period of an administrator password in days.
Expiration strategy	Defines the system action once a password expires: • *Block user* — The account is deactivated. • *Send factory password* — A temporary system-generated password is sent to the registered email.
Two-factor authentication (Re-authentication):	
Inactivity timeout (minutes)	The period of user inactivity after which the system requires re-authentication.
Auto logout without auth (days)	The number of days of continuous lack of login activity after which the account is automatically blocked.

It is not recommended to set parameter values below the system defaults.

After completing all fields, click the **Save** button.

High Security Level

When selecting the **High** security level, two additional configuration blocks become available in addition to the **Medium** level settings: **Disallowed password patterns** and **Disallowed password phrases**.

By default, some fields are pre-filled with recommended values. Parameters may be modified according to specific requirements.

It is not recommended to set parameter values below the system defaults.

The **Disallowed password patterns** block enables the configuration of character sequences that are restricted during password creation. These typically include commonly used, simple, and easily guessable sequences such as:

- *12345678*
- *qwerty*
- *1q2w3e*
- *zaq1*

To add a restricted pattern, enter the sequence into the **Add** field and click the icon. The sequence will be included in the list of prohibited patterns. The entire list can be cleared using the icon, or a single entry can be removed by double-clicking the icon. Additionally, a list of prohibited patterns can be uploaded as a file using the button.

The **Disallowed password phrases** block is used to restrict specific phrases during password creation.

A passphrase is a combination of several words, which is generally more secure than a single password. Passphrases are often easier to remember and provide enhanced length and security. For high reliability, the use of personal information in passphrases should be avoided.

The use of the following types of phrases is not recommended:

- *Smith 1999.07.05*
- *Admin password: 12345*

- *Name-2000*

To add a restricted phrase, enter it into the **Add** field and click the  icon. The phrase will be added to the prohibited list. The list can be cleared using the  icon, or a specific entry removed by double-clicking the  icon. Prohibited phrases can also be uploaded via a *.txt* or *.csv* file using the  button.

After completing all fields, click the **Save** button.

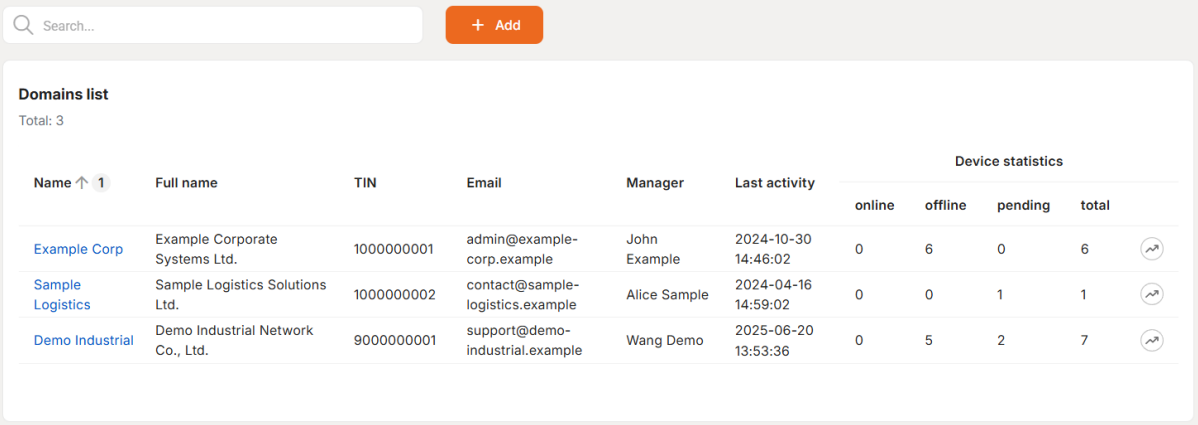


If a user attempts to set a password containing a prohibited pattern or phrase, the system will prevent the password from being saved.

5. Domains

A **Domain** represents an organizational unit used to manage network devices and configure specific access rights for company employees. It ensures the logical isolation of resources and administrative boundaries within the system.

This section displays a list of domains created by superusers. It provides general domain parameters, the timestamp of the most recent user login (tracking activity for any account regardless of its assigned role), and real-time operational status information for all connected devices.



5.1. New Domain

To create a new domain, click the 

button. This opens the new domain configuration page.

When defining a domain, the **Name** and **Email** fields are required. In the **Security profile** field, the global system profile (*default*) is selected automatically.

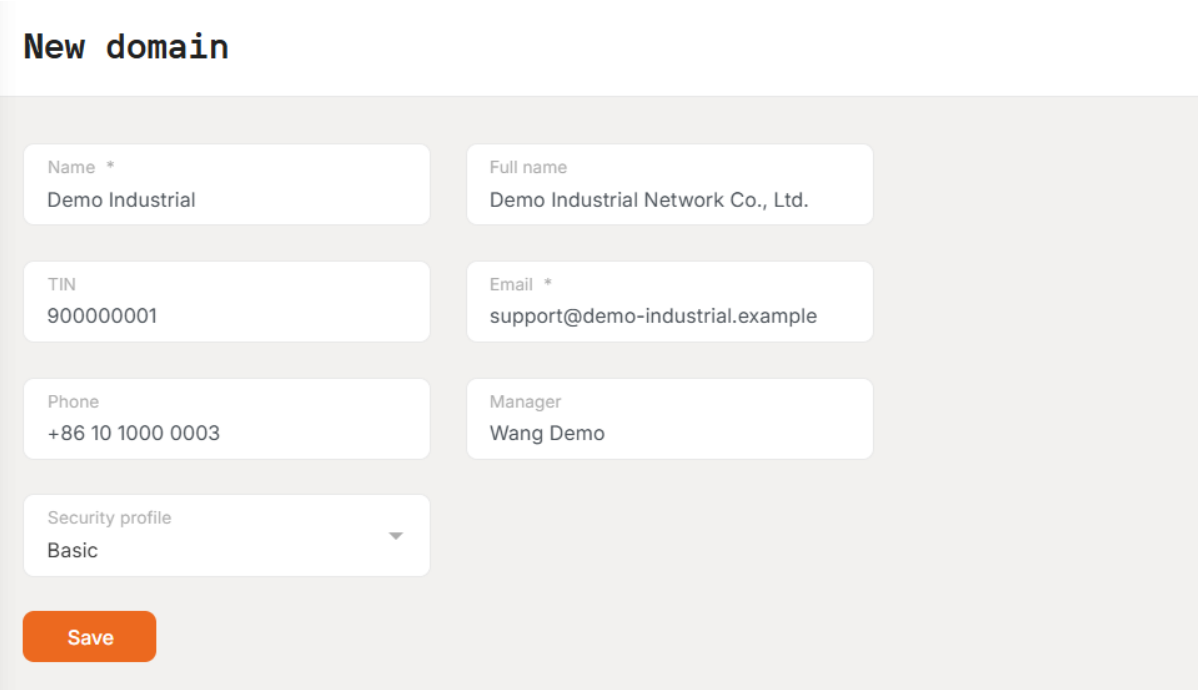


Table 3. Domain Parameters

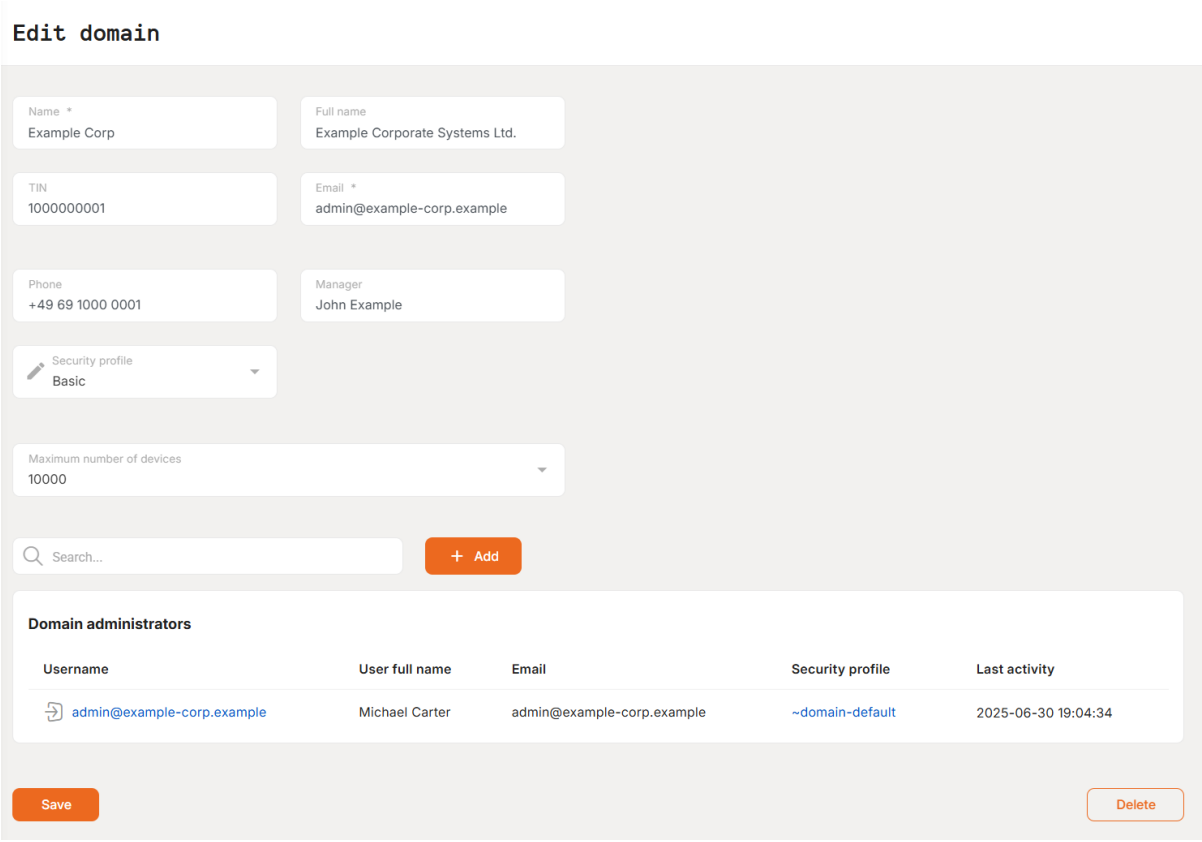
Field	Description
Name	Domain identifier (specified by the user; short company name recommended).
Full name	Full organizational name (specified by the user).
TIN *	Tax Identification Number.
Email *	Contact email address.
Phone *	Contact telephone number.
Manager *	Contact person or account manager name.
Security profile	Default security profile (selected from the provided list; *default* is assigned by system).

Fields marked with * are required when using the DRM cloud-based solution. As the cloud infrastructure is administered by Donyx technical support, this information is required for efficient client communication.

The selected security profile serves as the default for the domain. For detailed information on security profiles, refer to **Security** section.

5.2. Domain Editing

To edit a domain, click its name in the list. This opens a menu displaying current domain settings.



In addition to the basic parameters defined during creation, the domain editing menu provides advanced settings, such as the maximum number of devices and the creation of Domain Administrator profiles.

At least one **Domain Administrator** must be created for correct domain operation.

The **Maximum number of devices** field specifies the upper limit of equipment allowed within the domain. By default, this value is set to *unlimited*. To restrict the number of devices, select a specific value from the dropdown list.

The domain editing tab allows for adding an Administrator, viewing the current list of Domain Administrators, and editing their respective profiles.

A **Superuser** profile is not a domain user account. A separate profile is required to log in to a specific domain as a regular user.

5.3. Domain Administrator

To create a domain administrator, click the 

icon. In the **New administrator** menu, enter the profile details.

When creating a new domain administrator, the **Login**, **Email**, and **Password** fields are required. In the **Security profile** field, the domain security profile (*domain-default*) is selected by default; however, it can be replaced with any profile from the list.

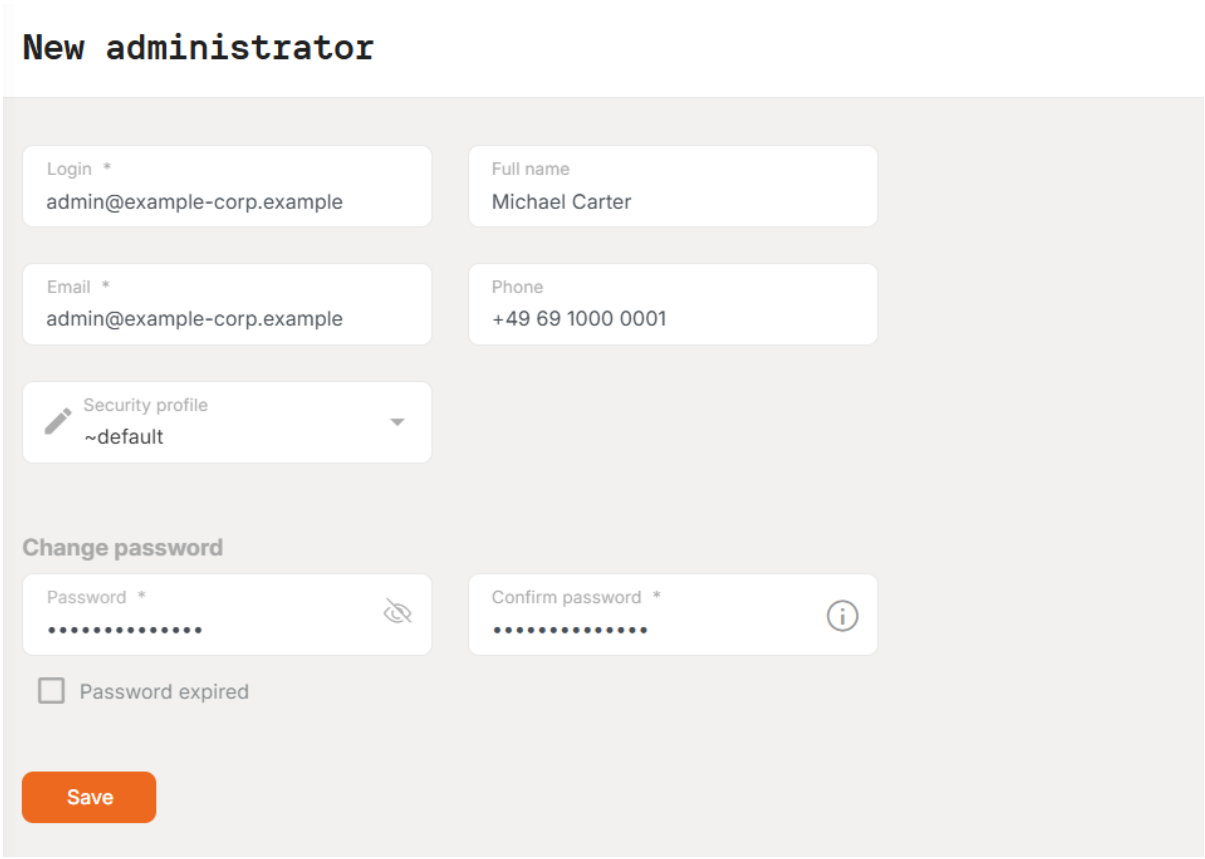


Table 4. Administrator Profile Settings

Field	Description
Login	Specified by the user.
Full name	Specified by the user.
Email	Employee's email address.
Phone	Specified by the user.

Security profile	*domain-default* (selected from the dropdown list).
Password	Specified by the user.
Repeat password	Specified by the user.

If required, the **Password expired** checkbox can be enabled to force a password change upon the user's next login.

Complete the required parameters and click the **Save** button.

5.4. Editing a Domain Administrator

To edit a domain administrator profile, navigate to the **Domains** tab.

1. Select the domain that contains the required administrator, then click the domain name to open the **Edit domain** menu.
2. From the list of domain administrators, select the specific user whose profile requires modification. This opens the **Edit administrator** menu.
3. Apply the necessary changes and click the **Save** button.

To delete an administrator profile, select the user's login from the domain administrators list and click **Delete** twice within the **Edit administrator** menu.

A **Superuser** profile is not a domain user account. A separate profile is required to log in to a specific domain as a regular user.

The **Superuser** can initiate domain administration directly. Within the **Edit domain** tab, click the icon next to any domain administrator's login. This action authenticates the Superuser as the selected Domain Administrator. Subsequent operations within the domain will be executed under the identity of that administrator. To return to the Superuser account, log out of the current session and re-authenticate as the Superuser.

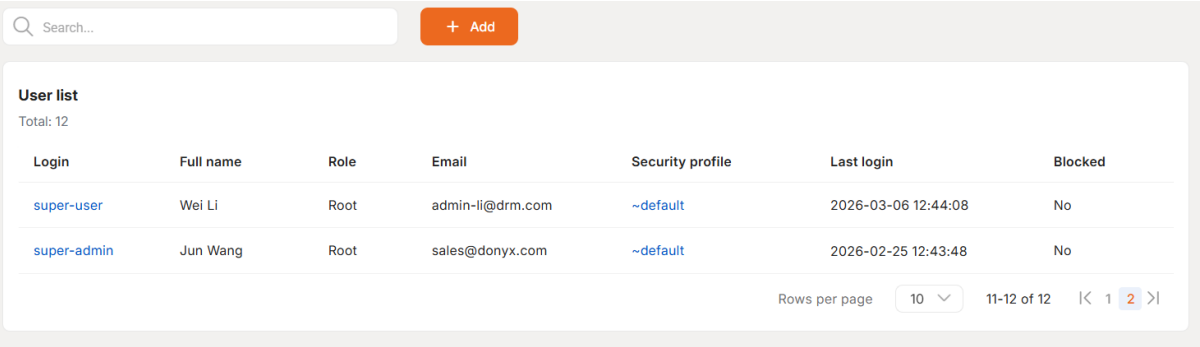
6. Users

6.1. Superusers

The **Superuser** (root) role represents the highest access level within the DRM system. Superusers are responsible for global system infrastructure management, including domain creation, security policy definition, and the administration of other high-level accounts.

The **Superusers** tab provides a centralized list of all created superuser accounts.

A **Superuser** profile is not a domain user account. A separate profile is required to log in to a specific domain as a regular user.



The following parameters are displayed for each superuser profile:

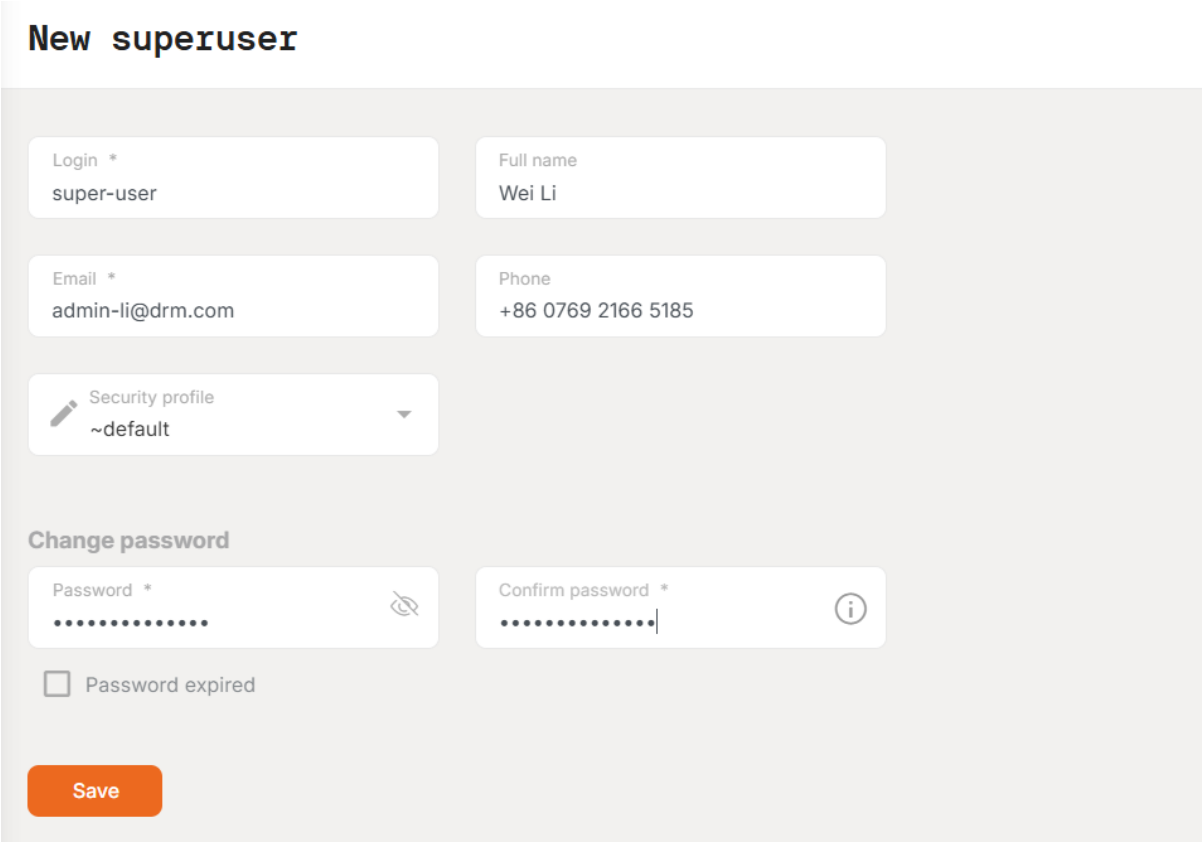
Table 5. Fields in the Superusers Tab

Field	Description
Login	The user's unique login identifier.
Full name	The user's full name.
Role	Access role (assigned as *Root* for this category).
Email	The user's registered email address.
Security profile	The security profile assigned to the account.
Last login	The timestamp of the most recent system authorization.
Blocked	The account blocking status.

The current active session account is excluded from the superuser list. If only one superuser exists in the system, the list will remain empty.

6.2. New Superuser

To add a superuser, click the + Add icon to open the **New Superuser** menu.



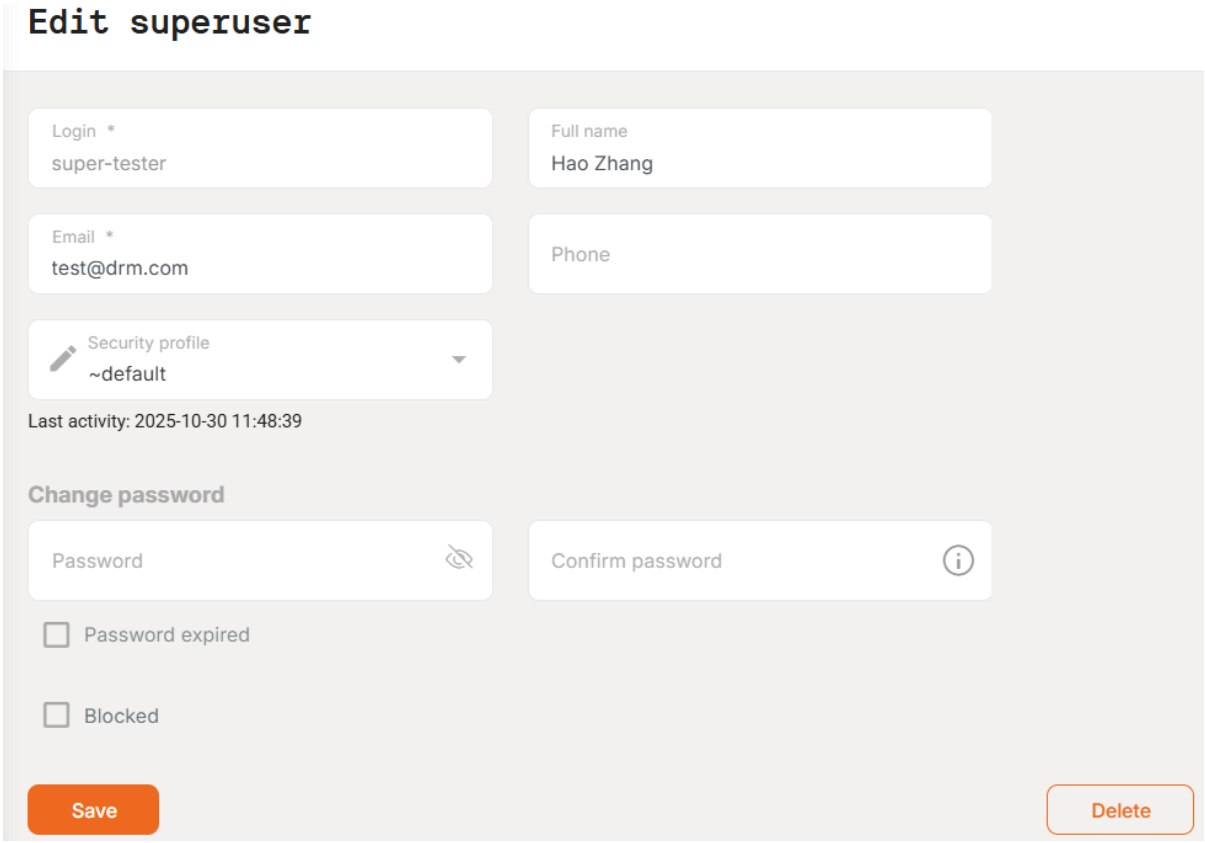
When creating a new **Superuser**, the **Login**, **Email**, and **Password** fields are required. In the **Security profile** field, the global security profile (*default*) is selected automatically; however, it can be replaced with any profile from the list.

If required, the **Password expired** checkbox can be enabled to force a password change upon the user's next login.

Complete the required parameters and click the **Save** button.

6.3. Editing a Superuser

To edit a superuser profile, navigate to the **Superusers** tab. Select the profile from the list and click the login identifier. This opens the **Edit Superuser** menu.



This menu allows for modifying personal data, changing the security profile, and deleting or blocking the user.

Changing the security profile automatically activates the **Password expired** option, which cannot be disabled. The user is required to update the password upon the next login after a profile change.

The default *root* superuser is assigned an extended password validity period.

If the security profile is modified, the password expiration period may be shortened. In such cases, the password must be updated promptly to prevent account lockout.

Unlocking a Superuser

To unlock a superuser account that has been blocked (due to password expiration or inactivity), navigate to the **Superuser** tab. Click the login of the blocked user. In the **Edit Superuser** menu, disable the **Blocked** option and click **Save**. The account will be restored to active status.

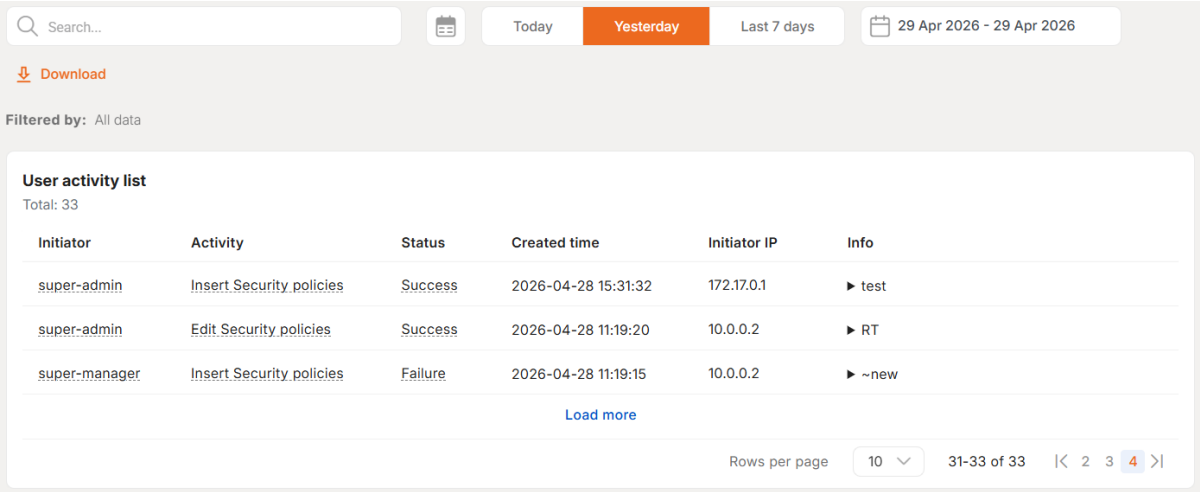
Deleting a Superuser

To remove a superuser profile, navigate to the **Superusers** tab. Select the account to be removed and click the login. In the **Edit Superuser** menu, click the **Delete** button, wait for it to turn red, and click it again to confirm.

After completing the required fields, click **Save**.

6.4. Logs

The **Logs** tab shows a record of all user activity within the system.



This section displays general details for each recorded event.

Table 6. User Activity List Parameters

Field	Description
Initiator	The login identifier of the user who performed the action.
Activity	The category or type of event.
Status	The outcome of the event (e.g., *Success* or *Error*).
Created time	The timestamp when the event was recorded.
Initiator IP	The IP address from which the user initiated the action.
Info	Technical details or additional data regarding the event.

The user activity log can be downloaded in *.csv* format. To do this, click the **Download** button.

Sorting and Filtering

The **User activity** list supports sorting and filtering by one or more parameters.

Sorting: Click the column header to apply sorting. A sorting icon and a priority number (if multiple columns are selected) will appear adjacent to the column name. Clicking the header again disables sorting for that specific column.

Filtering: Click on a specific value within the table to apply a filter. Filtering is supported for the **Initiator**, **Activity**, and **Status** parameters. Once applied, the active parameters and their values are displayed in the **Filtered by** field.

To reset all applied filters, click the **Clear** button.

Time Interval Selection

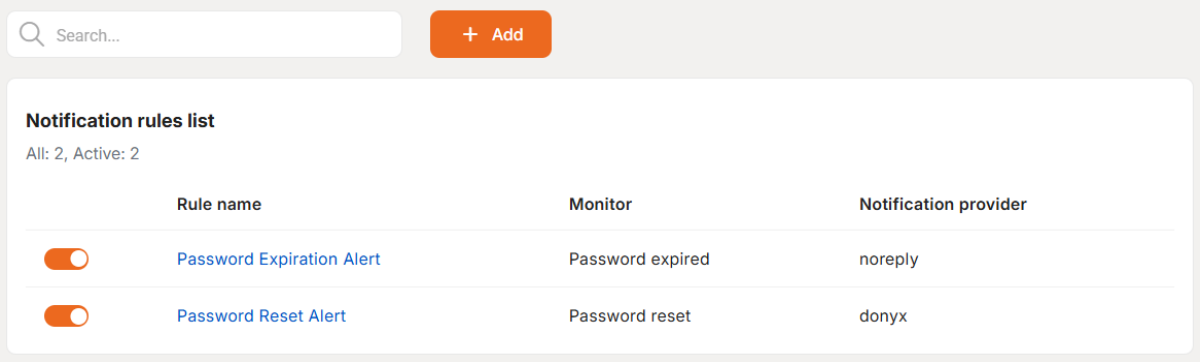
A specific time interval can be defined for displaying user activity records. To do this, click the icon. The interval can be selected from preset options (*Today*, *Yesterday*, *Week*) or specified manually.

By default, the list displays up to *2048* events. To retrieve earlier records, navigate to the end of the list and click **Load more**.

7. Notifications

The **Notification** tab lets you configure automated alerts. When a specific event is triggered, a message is sent via email.

The figure below illustrates the general view of the **Notification** tab.



This section displays a list of existing notification rules.

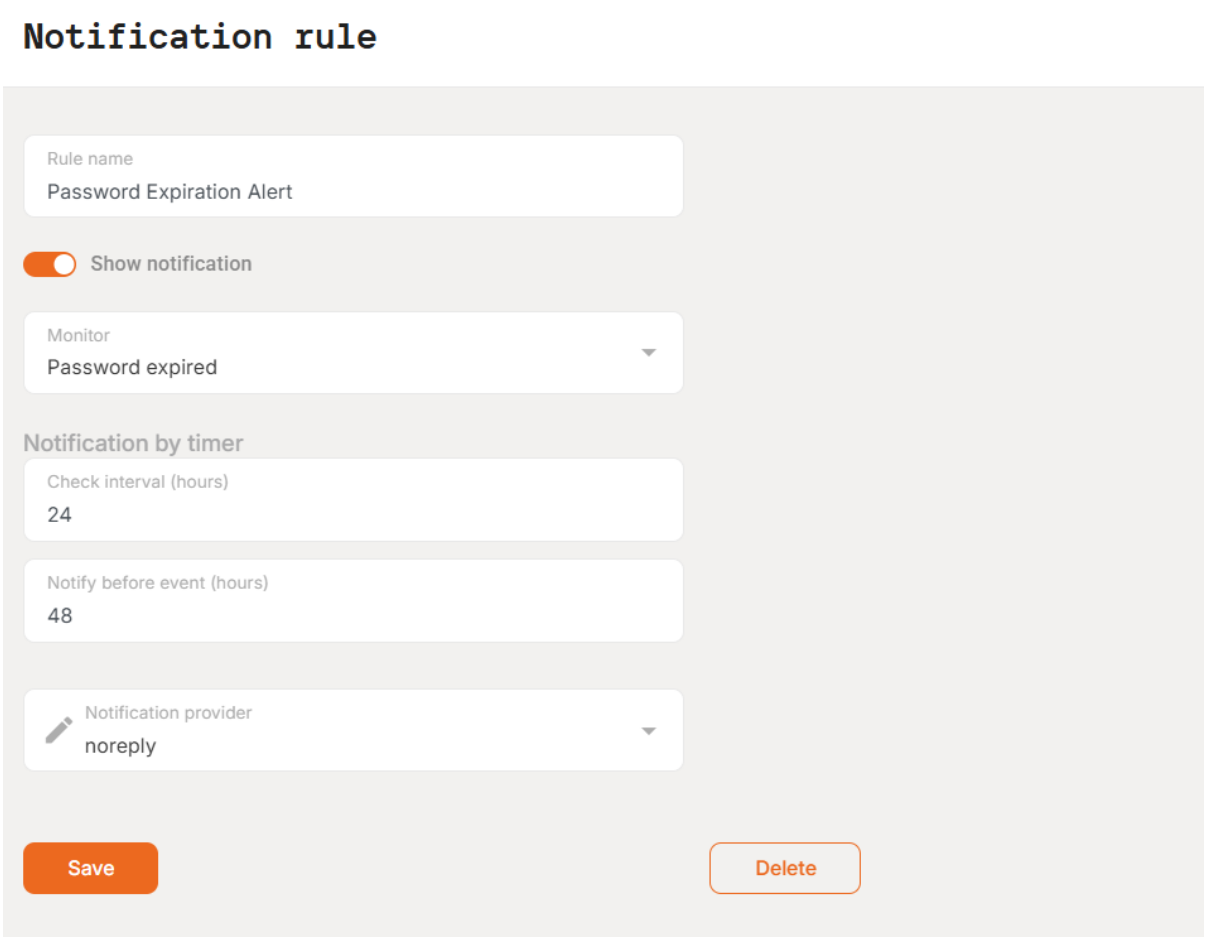
Table 7. Fields in the Notification Tab

Field	Description
Rule status switch	Indicates whether the rule is *active* or *inactive*.
Rule name	The identifier assigned to the notification rule.
Monitor	The monitoring category and specific event type that triggers the notification.
Notification provider	The technology or protocol utilized for message delivery.

To enable or disable an existing rule, use the toggle switch adjacent to the entry. A gray switch indicates that the rule is currently inactive.

7.1. New Notification rule

To add a new rule, click the + Add icon. This opens the **Notification rule** menu.



Configure the following parameters:

- Enter the rule identifier in the **Rule name** field.
- In the **Monitor** field, select an event or timer-based trigger. Two monitoring options are available for the Superuser *:
  - password reset (event notification);
  - password expired (timer notification).
- Specify the notification delivery method.
- Click the **Save** button.

* Notification rules for other event types are configured by Domain Administrators via the domain management interface. For detailed information, refer to the *Donyx DRM User's Guide*.

7.2. Editing a Notification Rule

To deactivate a rule, move the switch adjacent to the rule to the leftmost position; the switch will turn gray.

To modify a notification rule, select the required entry and click its name. In the **Notification rule** menu, apply the necessary changes and click the **Save** button.

To remove a rule, select the entry from the list and click its name. In the displayed menu, click **Delete** twice.

7.3. Notification provider (Delivery method)

If delivery methods have already been defined, select the required option from the **Notification provider** dropdown list. If no delivery methods exist, the list will be empty.

A new delivery method is created by clicking the + icon in the left part of the field and completing the required parameters.

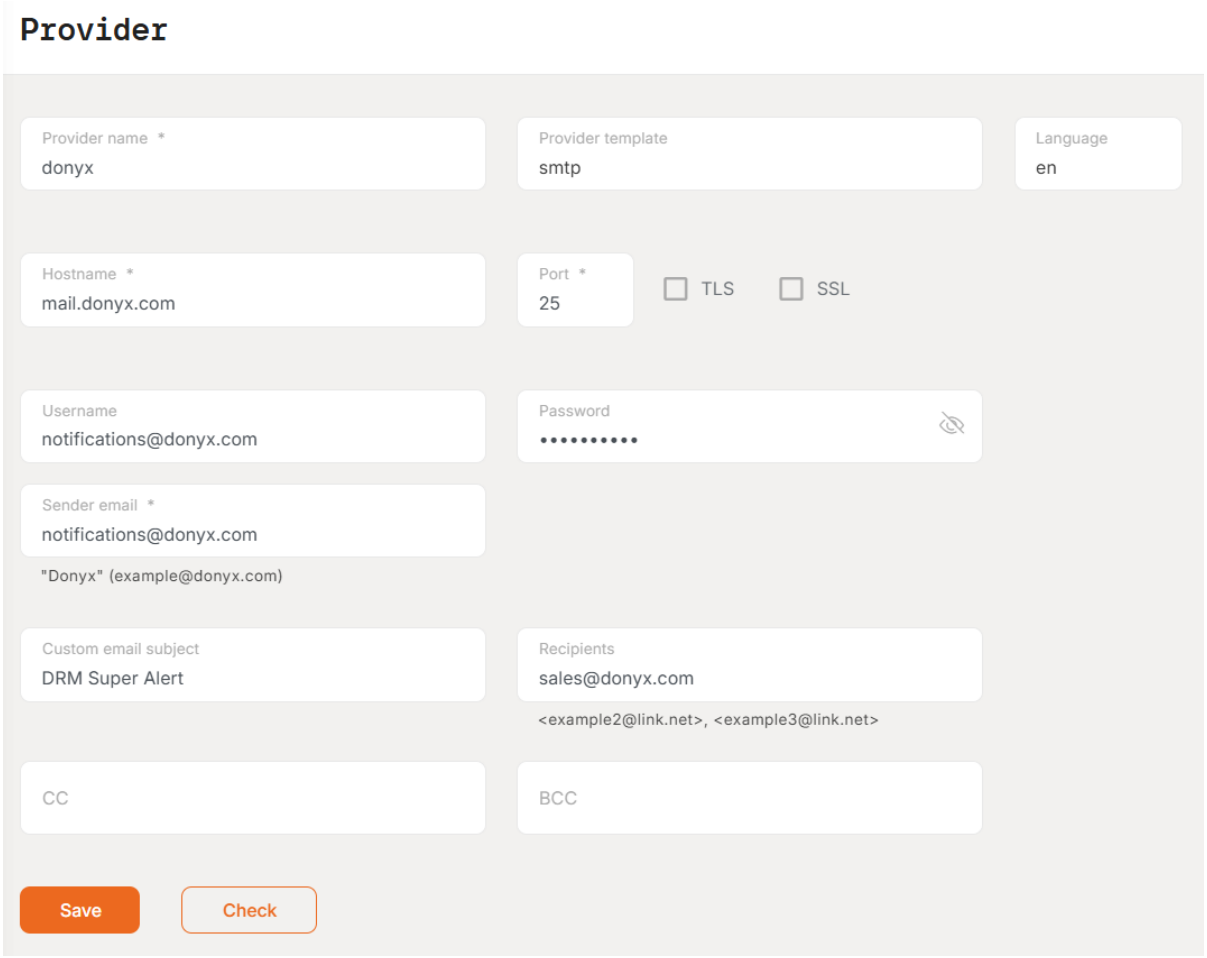


Table 8. Notification Provider Parameters

Field	Description
Provider name	The identifier for the notification method.
Provider template	*smtp* (the Superuser is restricted to the SMTP template).
Language	The language in which notifications will be generated. (EN).
Hostname *	Required. The SMTP server address.
Port *	Required. The SMTP server port. Typically, port *25* is used for unencrypted connections, while ports *465* or *587* are used for secure connections (SSL/TLS).
Username *	Authentication username for the SMTP server. This may be an email address or another identifier depending on server requirements.
Password *	Authentication password for the SMTP server.
Sender email *	Required. The email address from which notifications will be sent.
Custom email subject	The subject line for the notification email.
Recipients	Required. The email address(es) of the notification recipient(s). Multiple addresses must be separated by a comma or semicolon.
CC	Email address(es) for carbon copy (CC). Multiple addresses must be separated by a comma or semicolon.
BCC	Email address(es) for blind carbon copy (BCC). These recipients are not visible to others.

Fields marked with * must be populated with data provided by your IT department or Information Security service.

For the correct operation of notifications through the SMTP servers of certain email providers, additional account security settings may be required (such as generating an application-specific password or enabling access for third-party clients).

To verify the mail agent's functionality and the accuracy of the settings, click the **Check** button. A test email will be sent to the addresses specified in the **Recipients** field.

7.4. Editing a Notification Delivery Method

To edit a delivery method, select the rule utilizing it and click its name. In the **Notification rule** menu, click the icon in the **Notification provider** field. In the **Provider** menu, apply the necessary modifications (refer to the "Notification provider" section) and click the **Save** button.

A notification delivery method may be deleted only if it is not currently assigned to any active rule. To delete it, click the **Delete** button in the **Provider** menu, wait for it to turn red, and click it again to confirm.

If the **Delete** button is not displayed in the menu, the delivery method is currently in use and cannot be removed.

Notification delivery methods created by the Superuser are not shared with domains.

When performing domain administration (as a Domain Administrator), notification delivery methods must be configured independently.

8. Infrastructure

8.1. Firmware (Cloud only)

This section is not available in the on-premises version.

This section provides centralized management of software and firmware for the DRM system. After software files are uploaded, the system automatically verifies their status every hour to ensure all packages remain valid and ready for remote equipment updates.

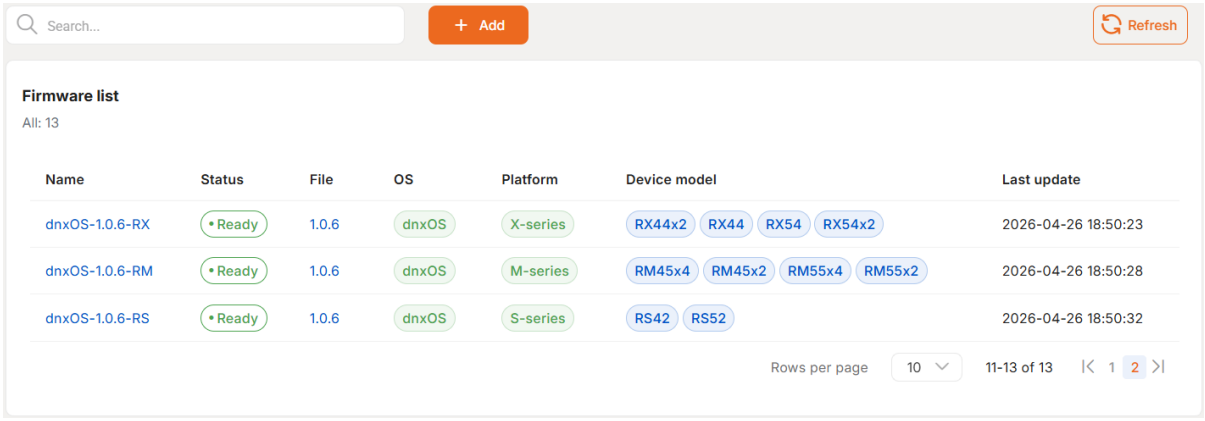


Table 9. Fields in the Firmware Tab

Field	Description
Name	Firmware filename (specified by the user).
Status	Current software validity status.
File	Software version identifier.
OS	Name of the operating system for which the firmware is intended (populated automatically).
Platform	Hardware series compatible with the software.
Device model	Specific equipment model for which the firmware is intended (specified by the user).
Last update	Timestamp of the most recent software update.

8.2. New Firmware

To add software to the list, click the + Add icon. This opens the **Rule for uploading new firmware** configuration page.



All fields are required when creating a new rule for uploading current software.

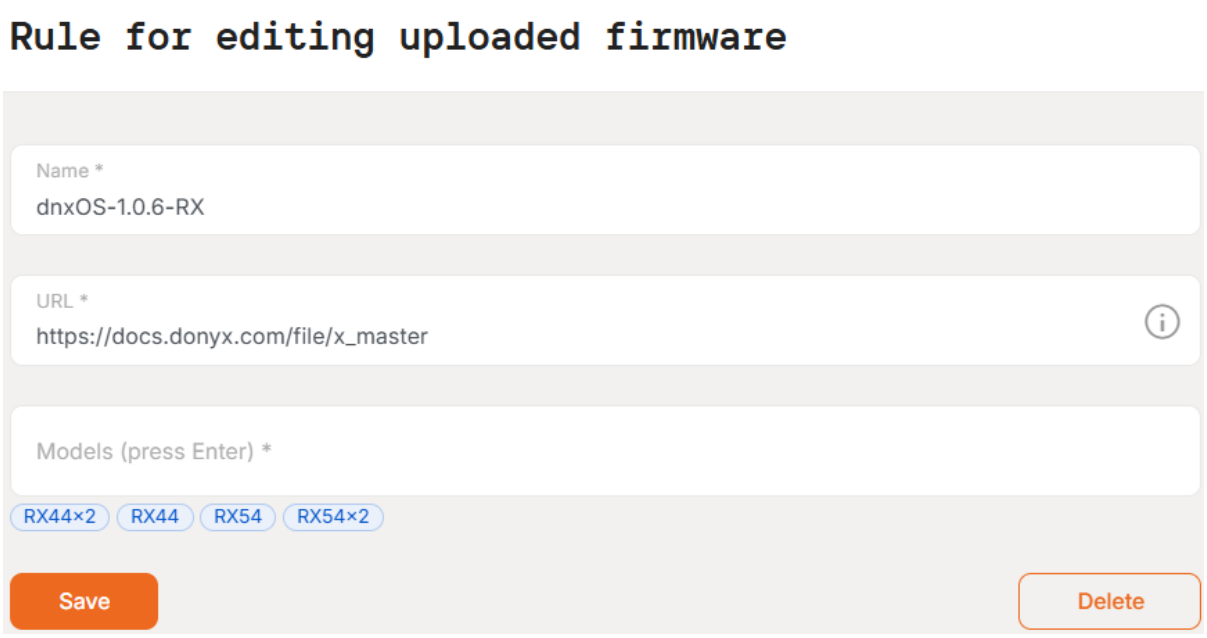
Table 10. Firmware List Parameters

Field	Description
Name	Firmware filename (specified by the user).
URL	The direct link to the firmware file.
Device model	Specific equipment model for which the firmware is intended (specified by the user).

Ensure the correct equipment model name is entered. If the model is specified incorrectly, the corresponding devices will not receive notifications regarding new software availability.

8.3. Editing a Firmware Rule

To modify a firmware rule, select the software entry from the list and click its name. This opens the editing page for the software rule.



Modify the required fields as necessary.

To add equipment models, enter the model name into the corresponding field and press **Enter**.

To remove a model from the list, hover the mouse cursor over the model name. Once the name turns red, click it to remove the device from the list.

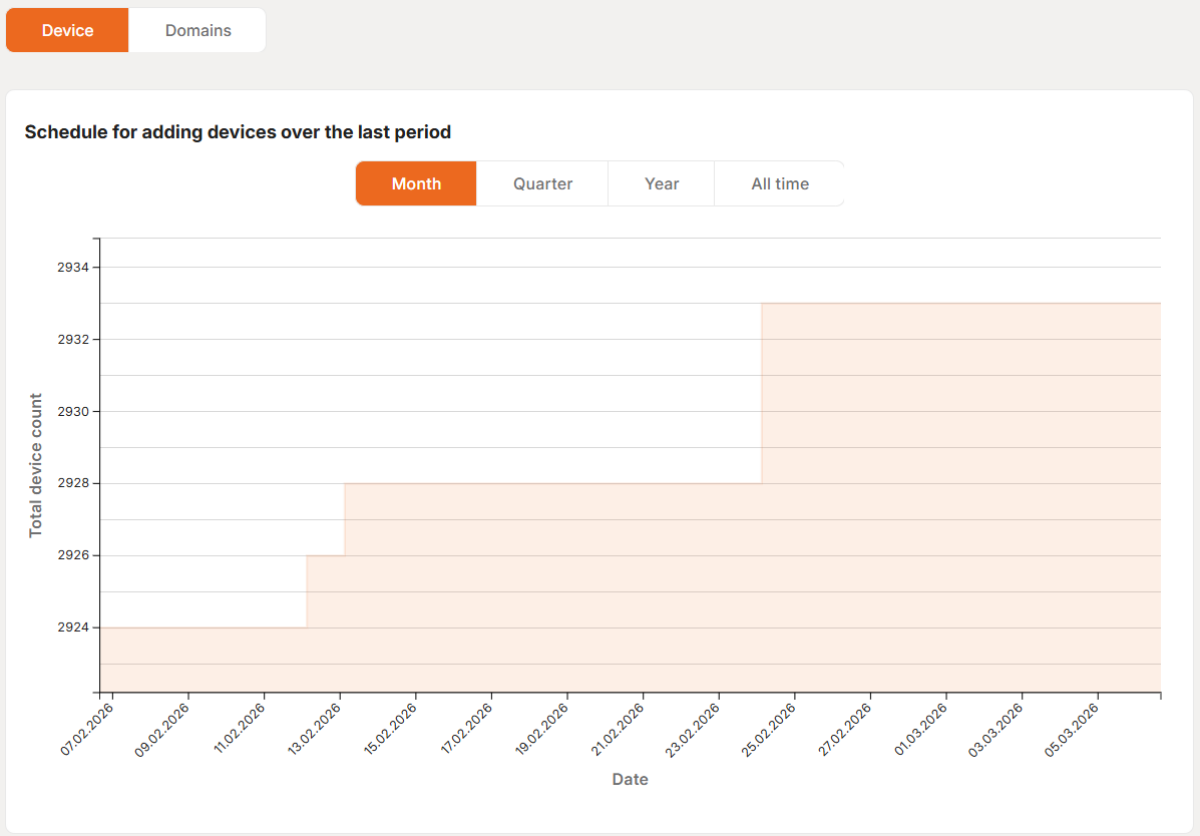
After applying the necessary adjustments, click the **Save** button.

Deleting a Firmware Rule

To delete a firmware rule, select the software entry from the list and click its name. In the displayed editing page, click the **Delete** button, wait for it to turn red, and click it again to confirm the deletion.

9. Statistics

The **Statistics** section is accessed by clicking the corresponding icon in the top-right corner of the interface.



This section provides analytical data regarding the number of domains and devices within the system. The graphical visualizations

- **Schedule for adding devices over the last period:** Displays the correlation between **Date** and the **Total device count**.
- **Schedule of domain additions over the last period:** Displays the correlation between **Date** and the **Total domains count**.

Statistical data can be viewed for specific timeframes, including monthly, quarterly, yearly intervals, or for the entire operational period.

10. Account Management

The user settings section is located in the top-right corner of the web interface. To access the section, click the icon.

The web interface theme is toggled via the icon.

User profile data is managed in the **Profile** sub-section. The following fields are available for modification:

- Full name.
- Email address.
- Contact phone number.
- New password *.

* The password can only be changed once every 5 minutes.

This section also allows users to delete their own account. To perform this action, click the **Delete** button five times; the profile will then be removed.

After completing the fields, click **Save**.

The **DRM** system version number is displayed within the profile editing menu. It is located in the bottom-left corner of the screen.

11. Customer Support

Website	donyx.com
Email	support@donyx.com